

Fig.1

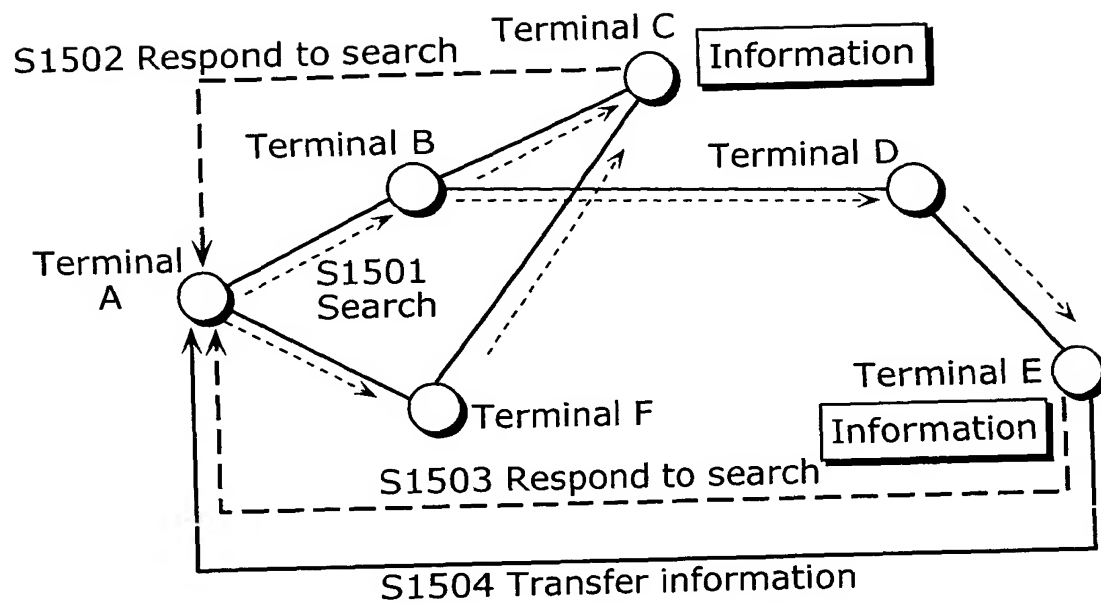


Fig.2

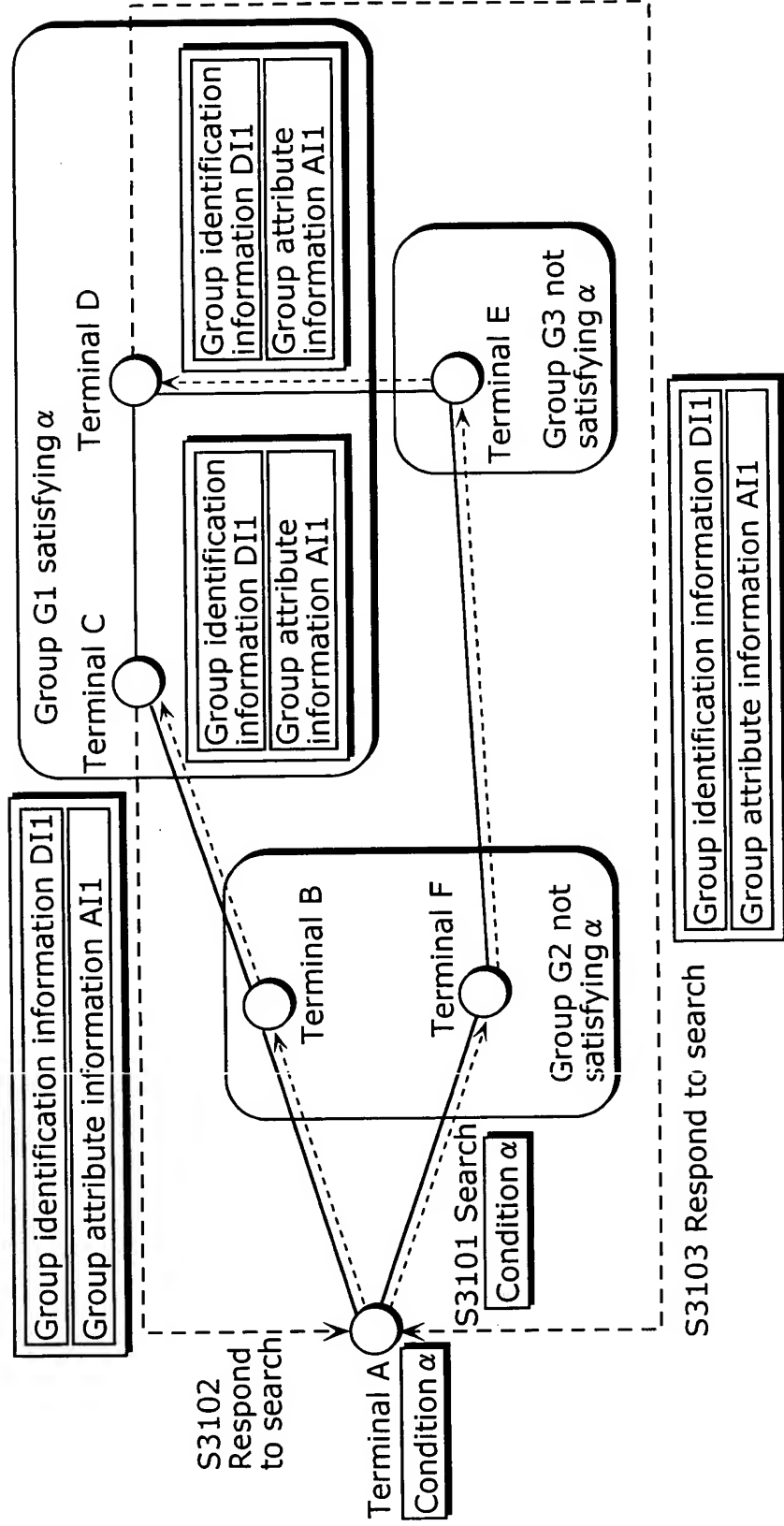
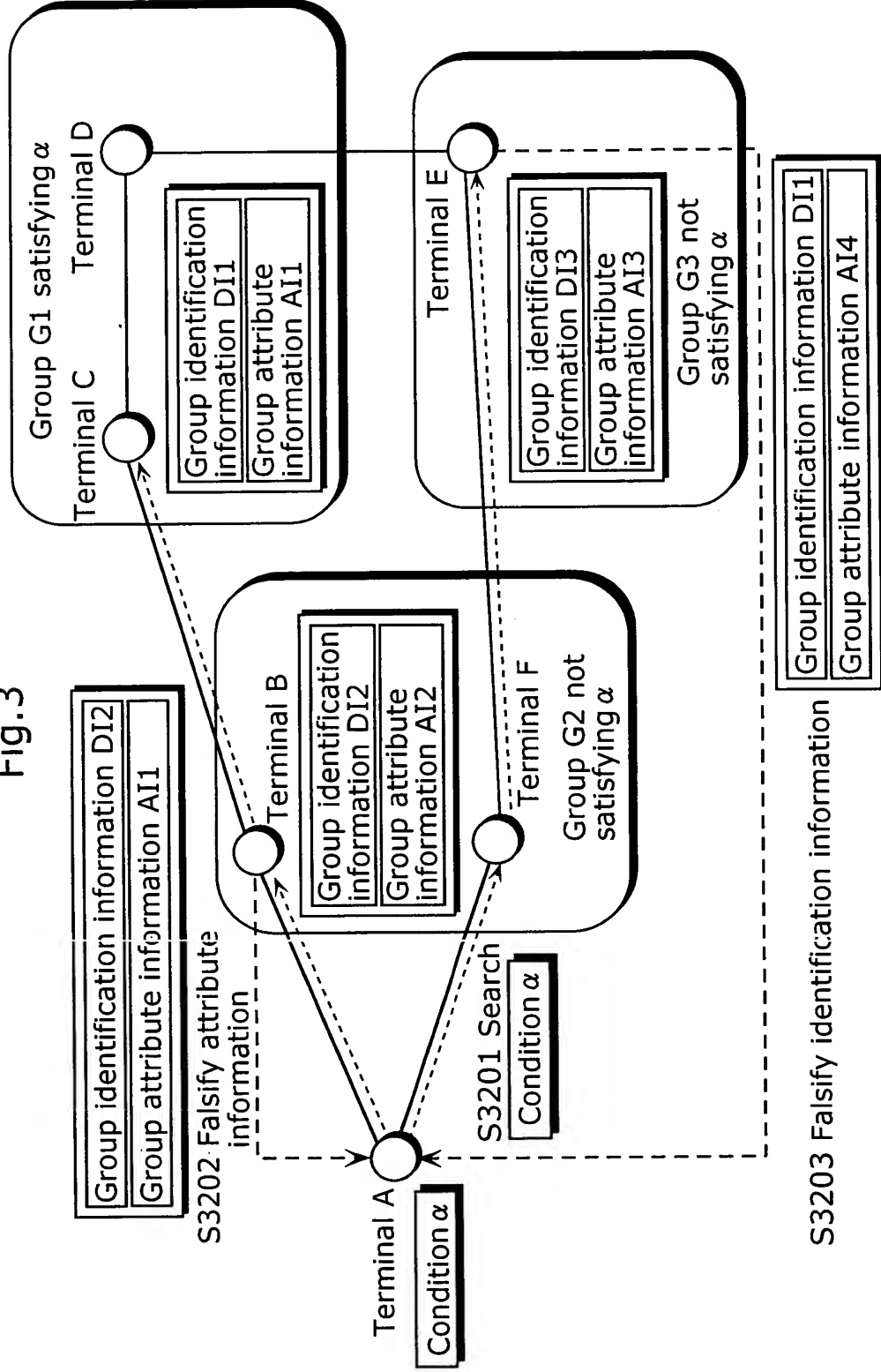


Fig.3



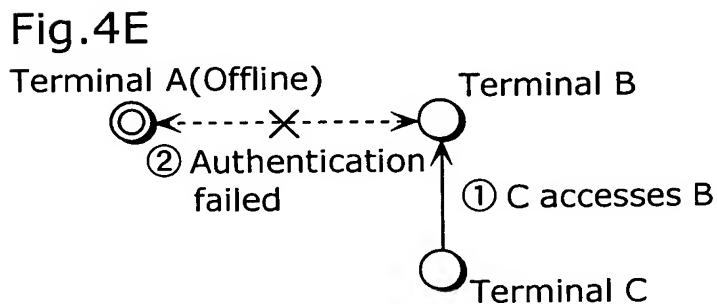
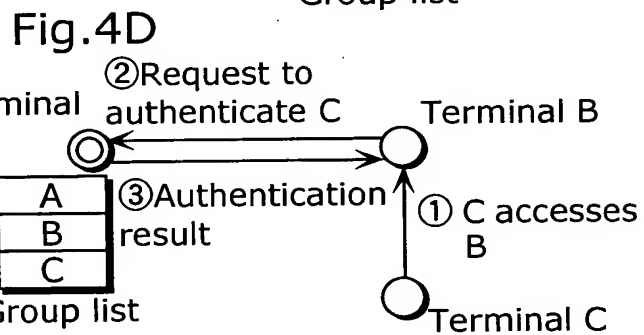
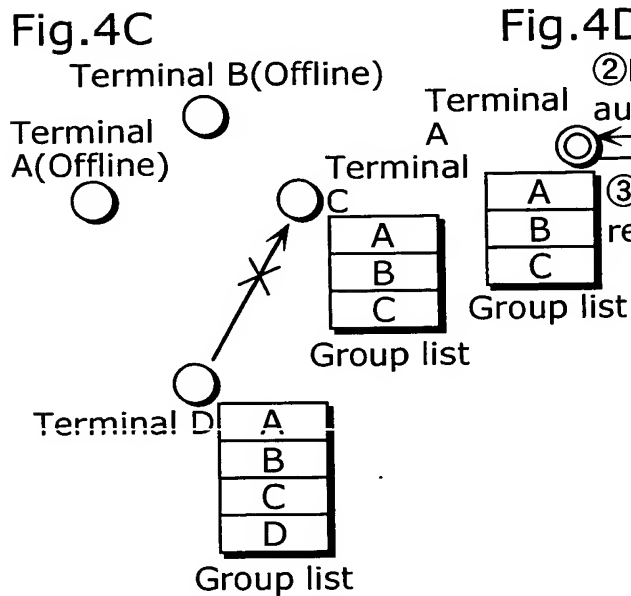
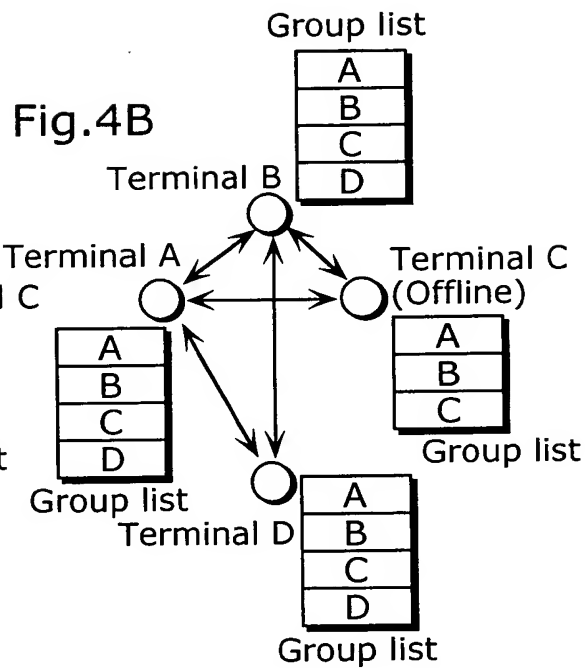
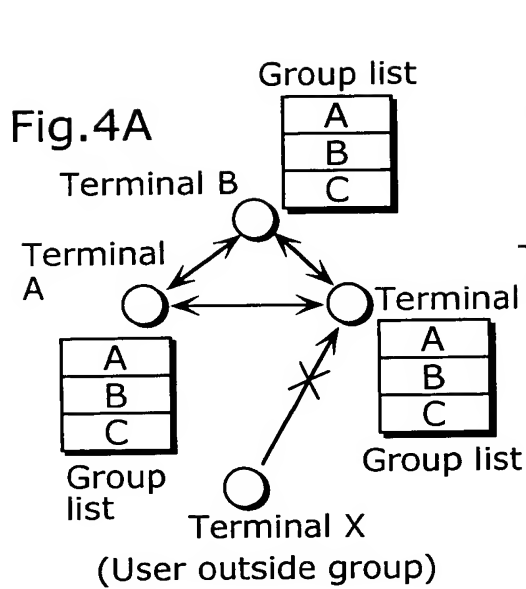


Fig.5A Expired participant lists:

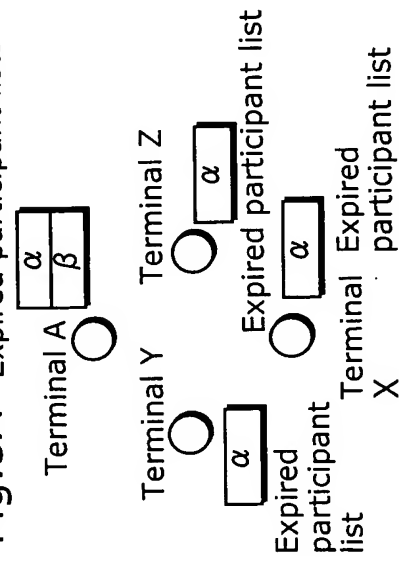


Fig.5B Expired participant lists

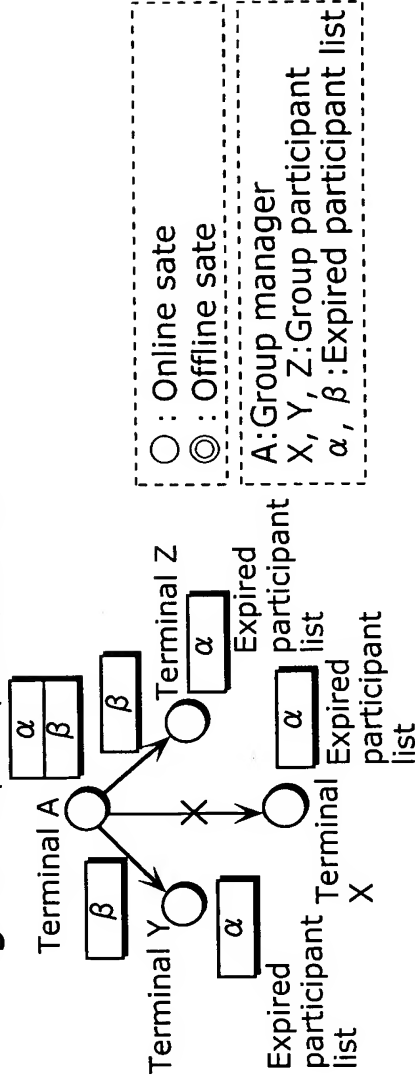


Fig.5C Expired participant lists

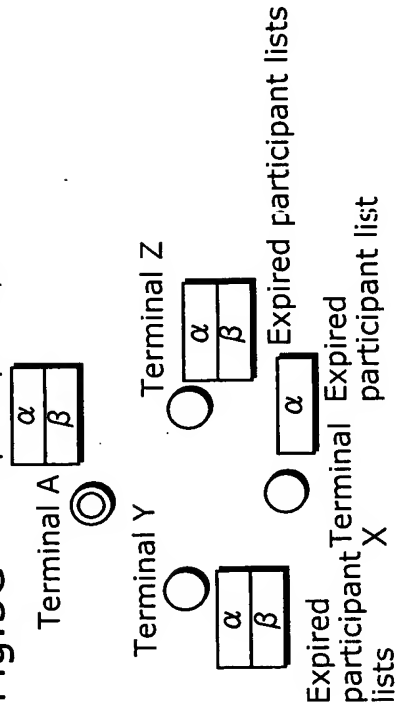


Fig.5D Expired participant lists

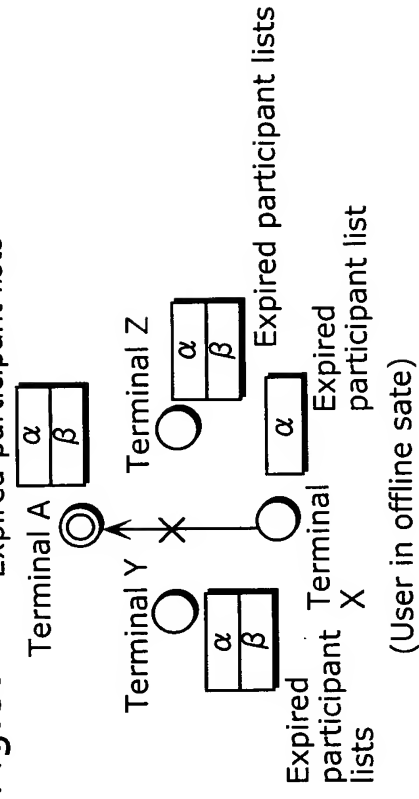


Fig.6

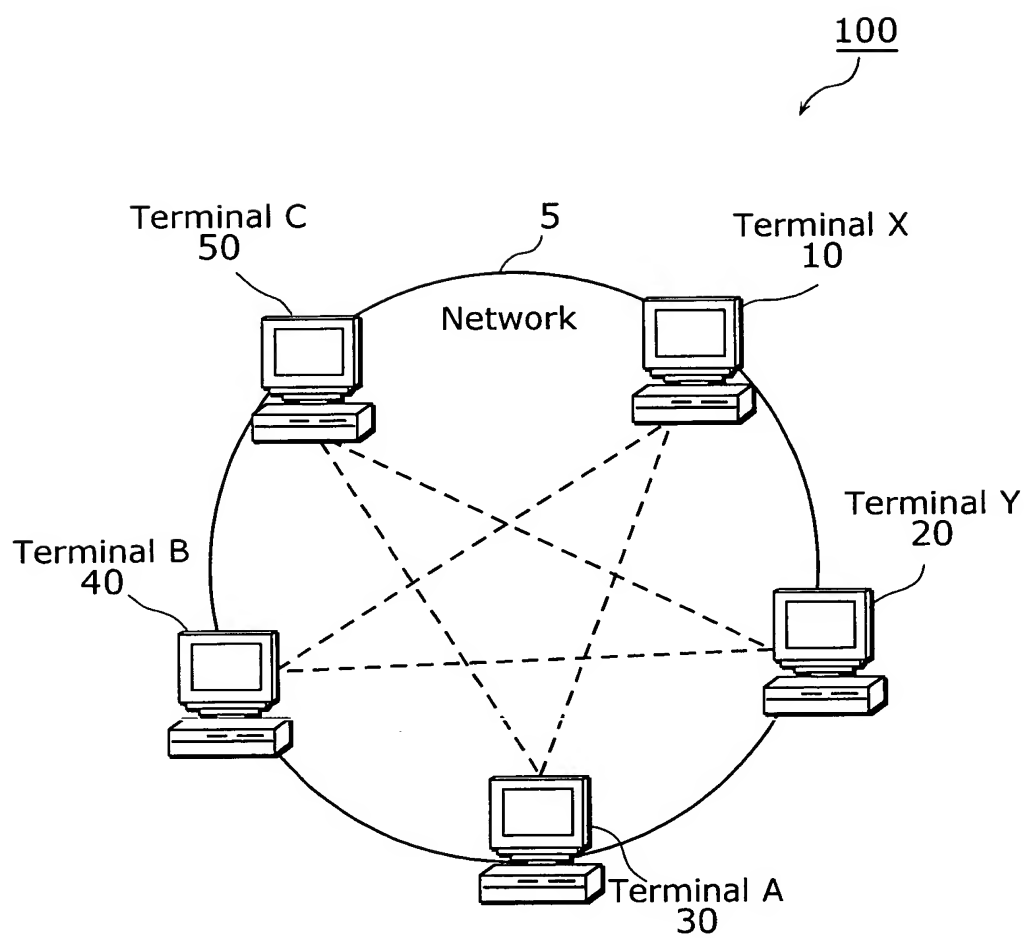


Fig.7

Expired participant list ID
Date of issue
Expiration date
ID of preparer of expired participant list
Expired participant ID list
Expired participant ID
Expired participant ID
⋮
Expired participant ID
Signature created by using group private key

Fig.8A

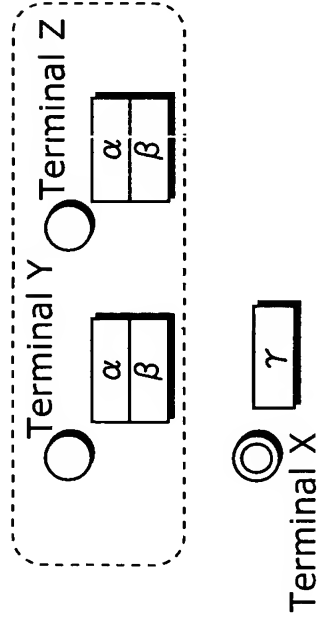


Fig.8B

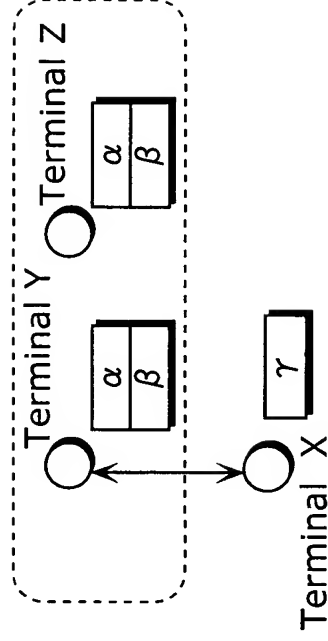


Fig.8C

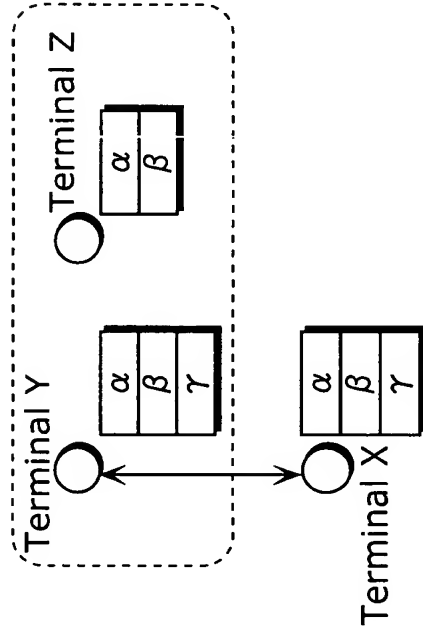


Fig.8D

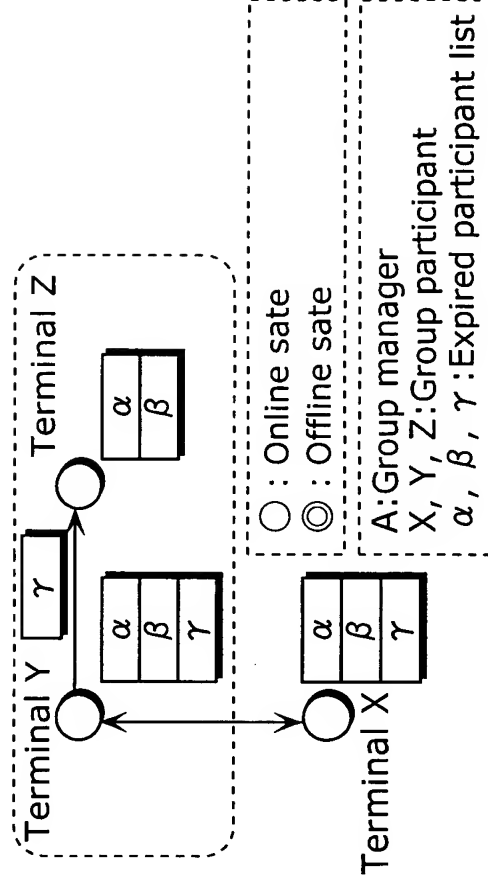




Fig.9

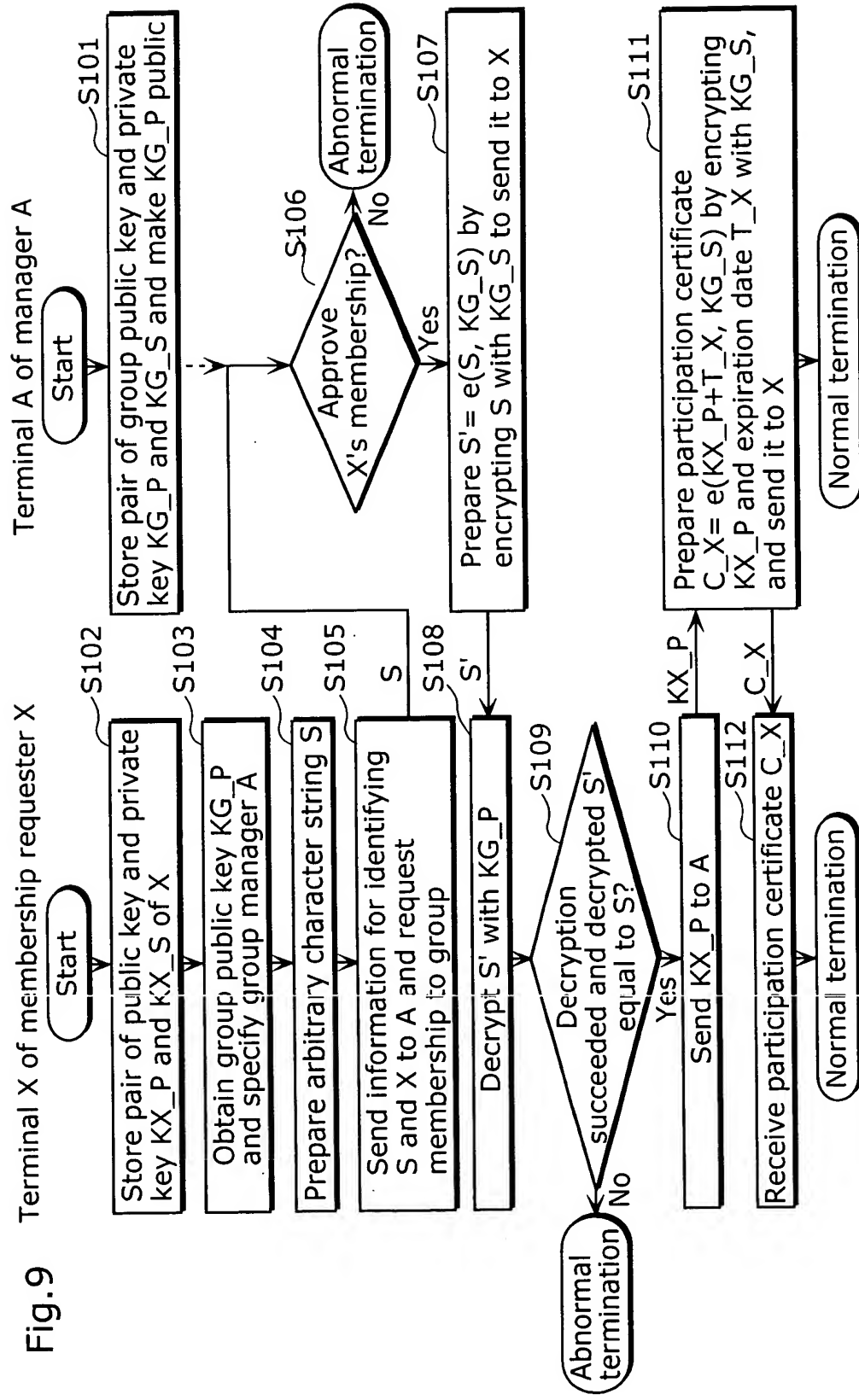
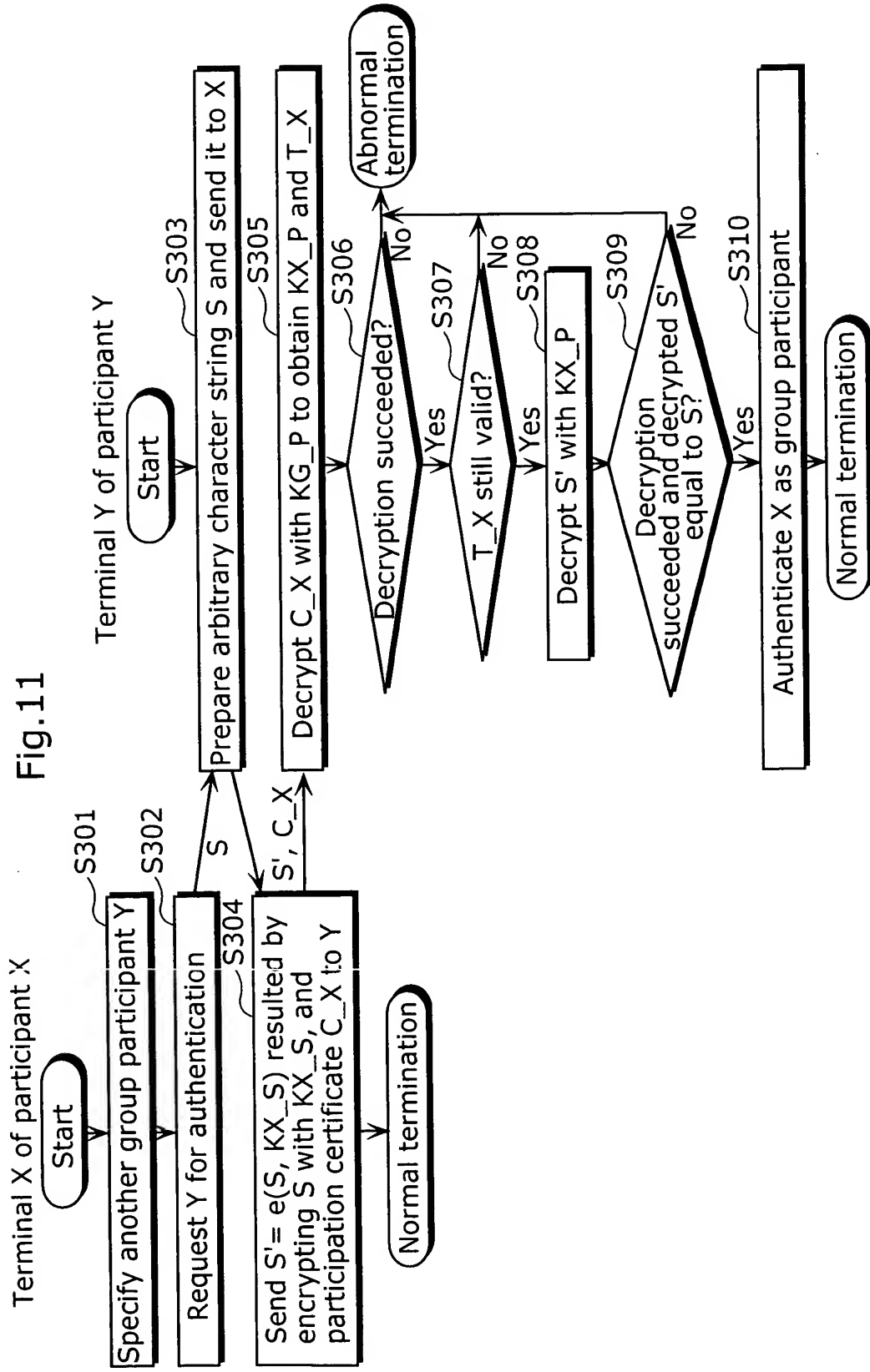


Fig.10

KX\_P:Public key of X  
KX\_S:Private key of X  
KG\_P:Group public key  
 $C_X = e(KX_P + T_X, KG_S)$ :Group participation certificate of X



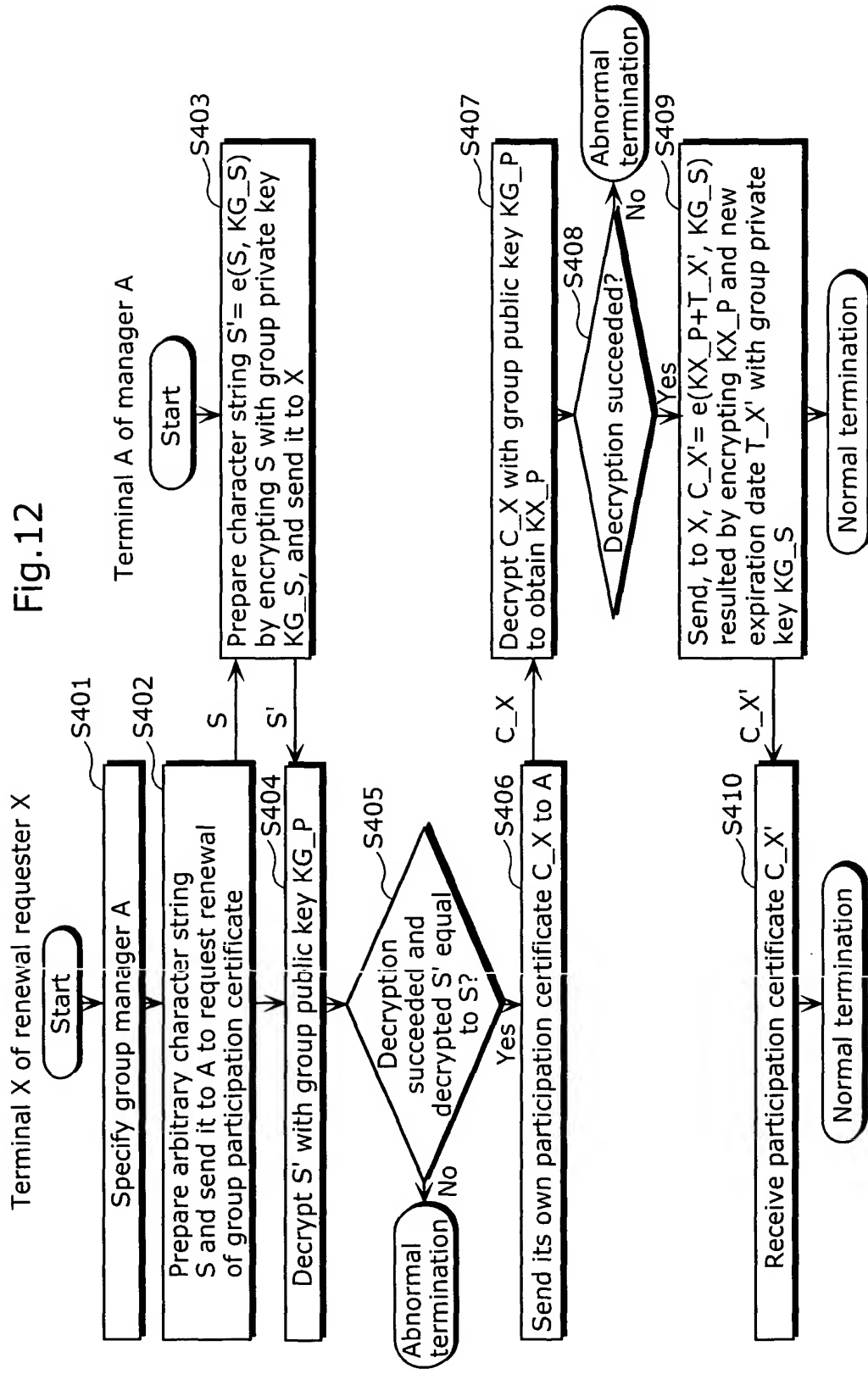


Fig.13

Expired participant list ID
Date of issue
Expiration date
ID of preparer of expired participant list
Expired participant ID list
Expired participant ID
Expired participant ID
⋮
Expired participant ID
Participation certificate issue permit
Signature created by using issuer's private key

Fig.14

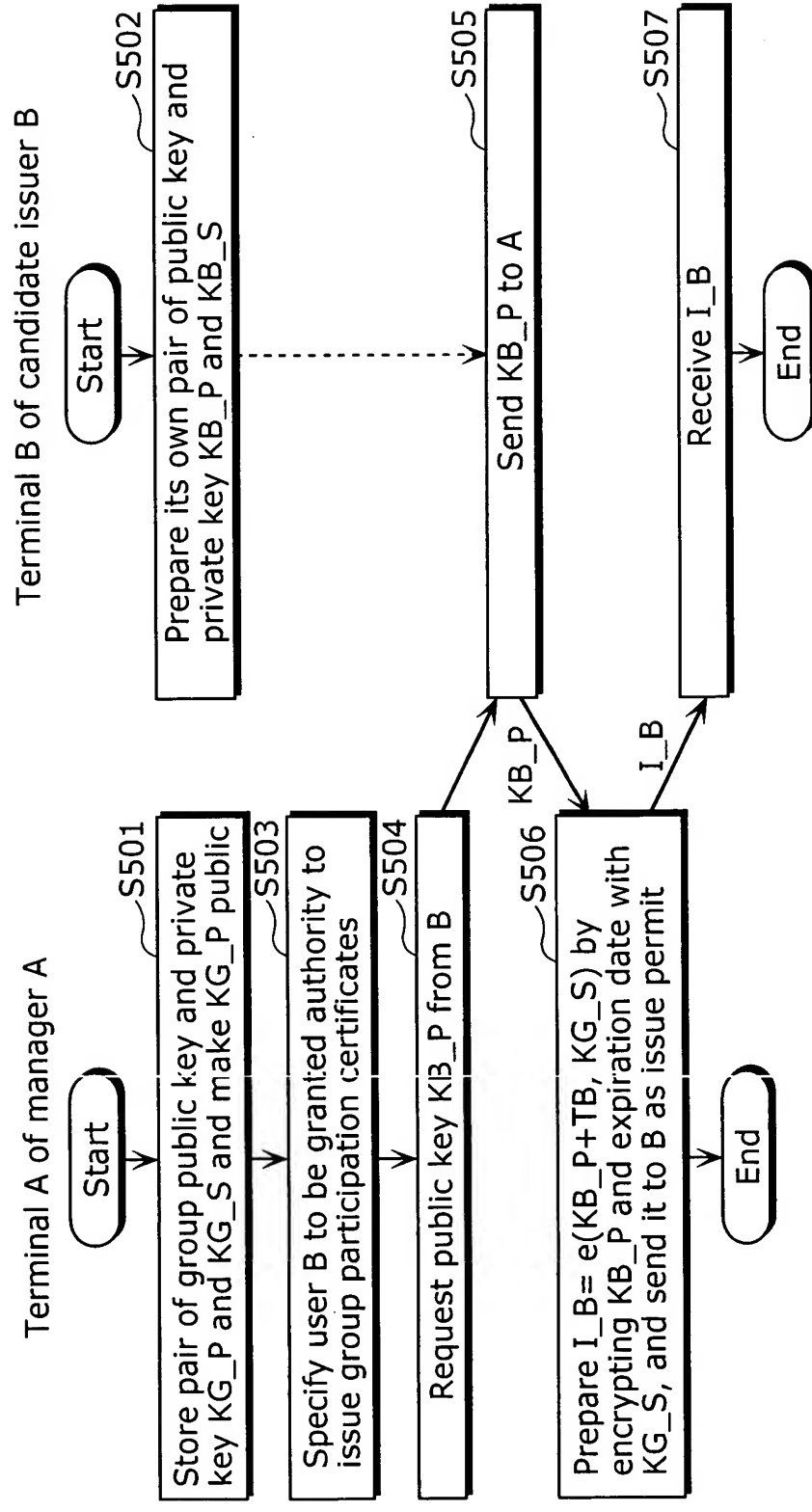


Fig.15

KB\_P:Public key of B  
KB\_S:Private key of B  
KG\_P:Group public key  
 $I_B = e(KB_P + T_B, KG_S)$   
:Group participation certificate issue permit of B

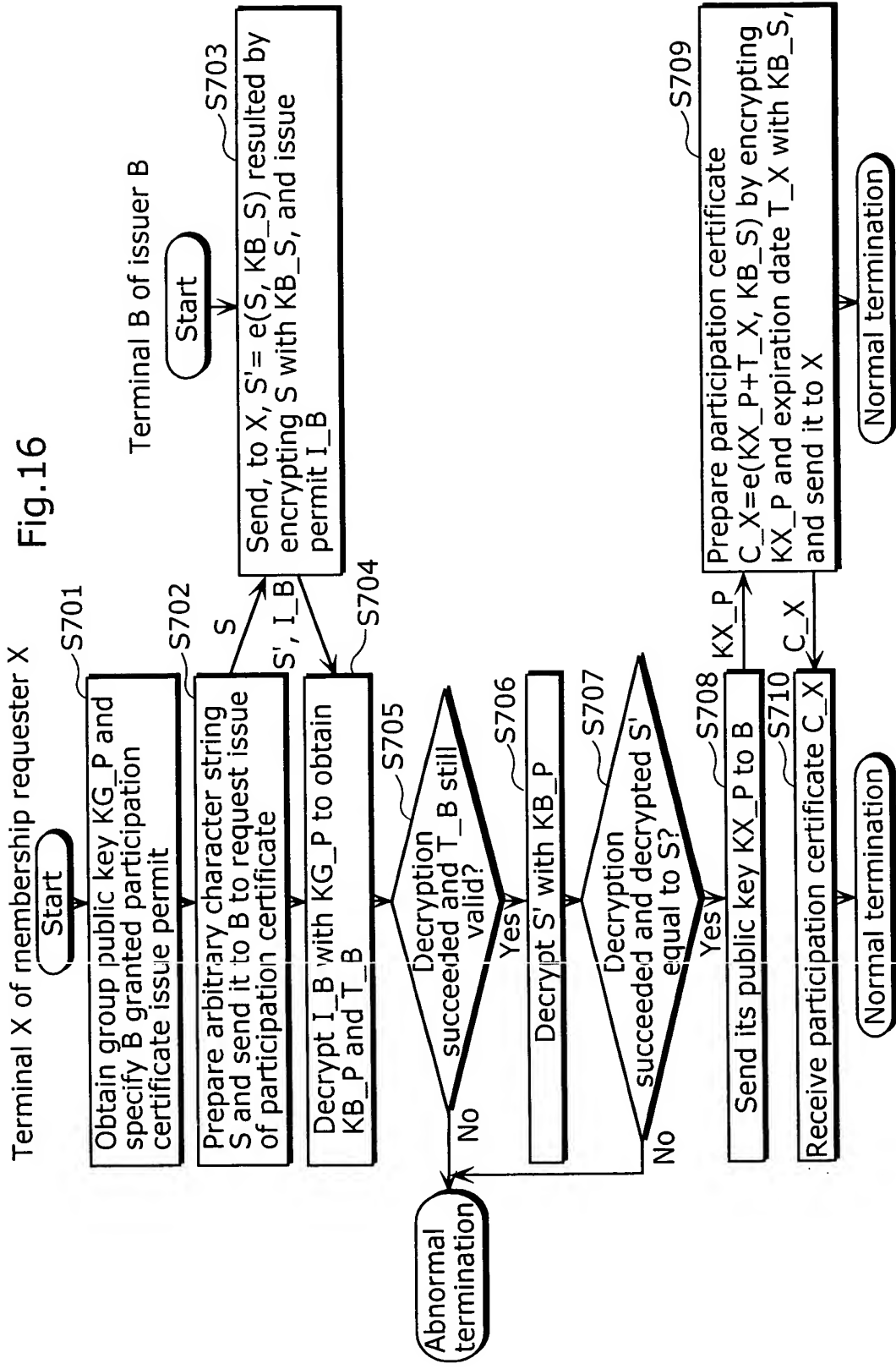


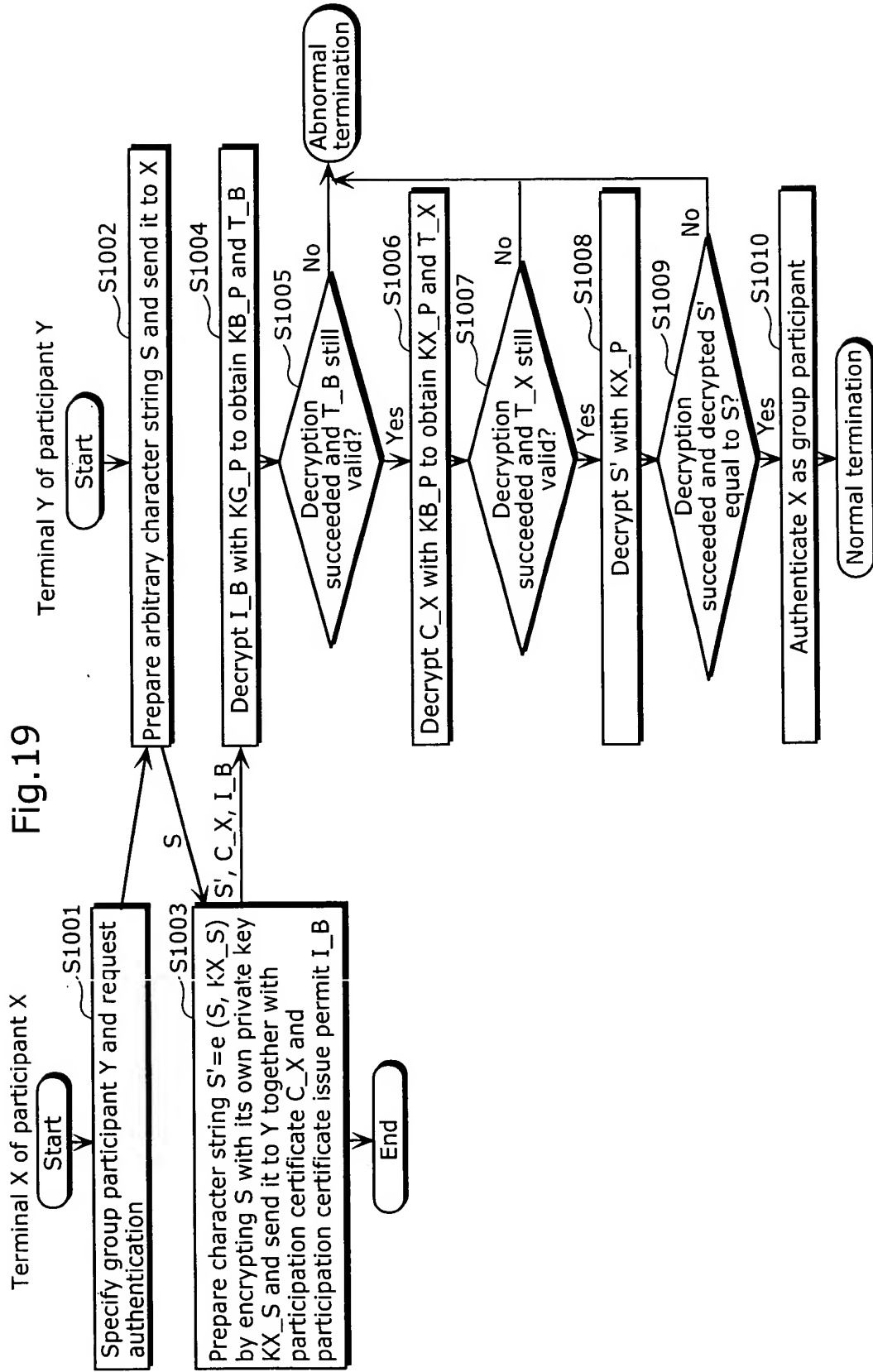


Fig.17

KX\_P:Public key of X  
KX\_S:Private key of X  
KG\_P:Group public key  
 $I_B = e(KB_P + T_B, KG_S)$   
:Group participation certificate issue permit of B  
 $C_X = e(KX_P + T_X, KB_S)$ :Group participation certificate of X

Fig.18

KY\_P:Public key of Y  
KY\_S:Private key of Y  
KG\_P:Group public key  
 $I_C = e(KC_P + T_C, KG_S)$   
:Group participation certificate issue permit of another issuer C  
 $C_Y = e(KX_P + T_X, KB_S)$   
:Group participation certificate of Y issued by C



Terminal X of participation certificate renewal requester X

Fig.20

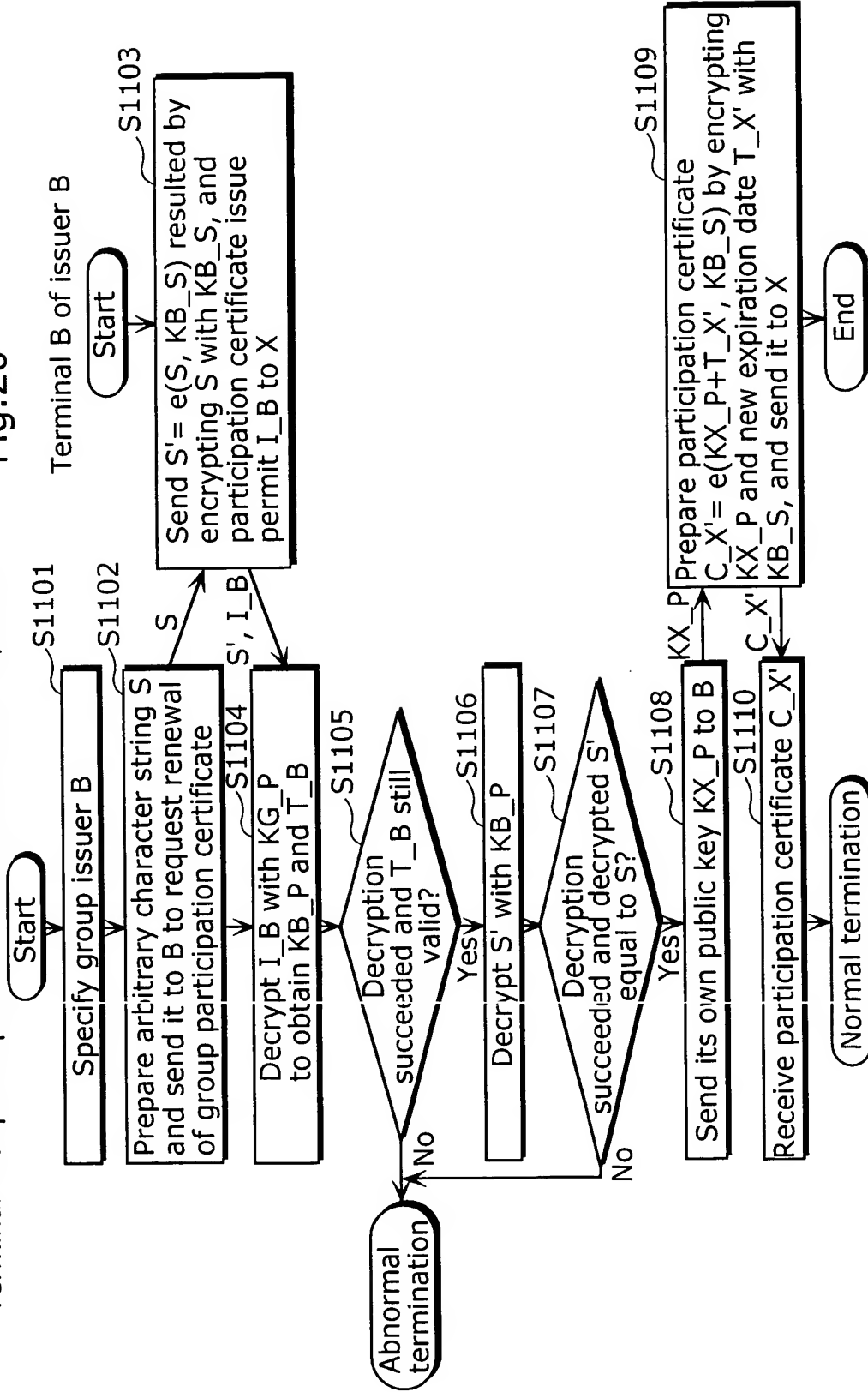


Fig.21

KX\_P:Public key of X  
KX\_S:Private key of X  
KG\_P:Group public key  
 $I_B = e(KB_P + T_B, KG_S)$   
:Group participation certificate issue permit of B  
 $C_X = e(KX_P + T_X', KB_S)$ :Group participation certificate of X

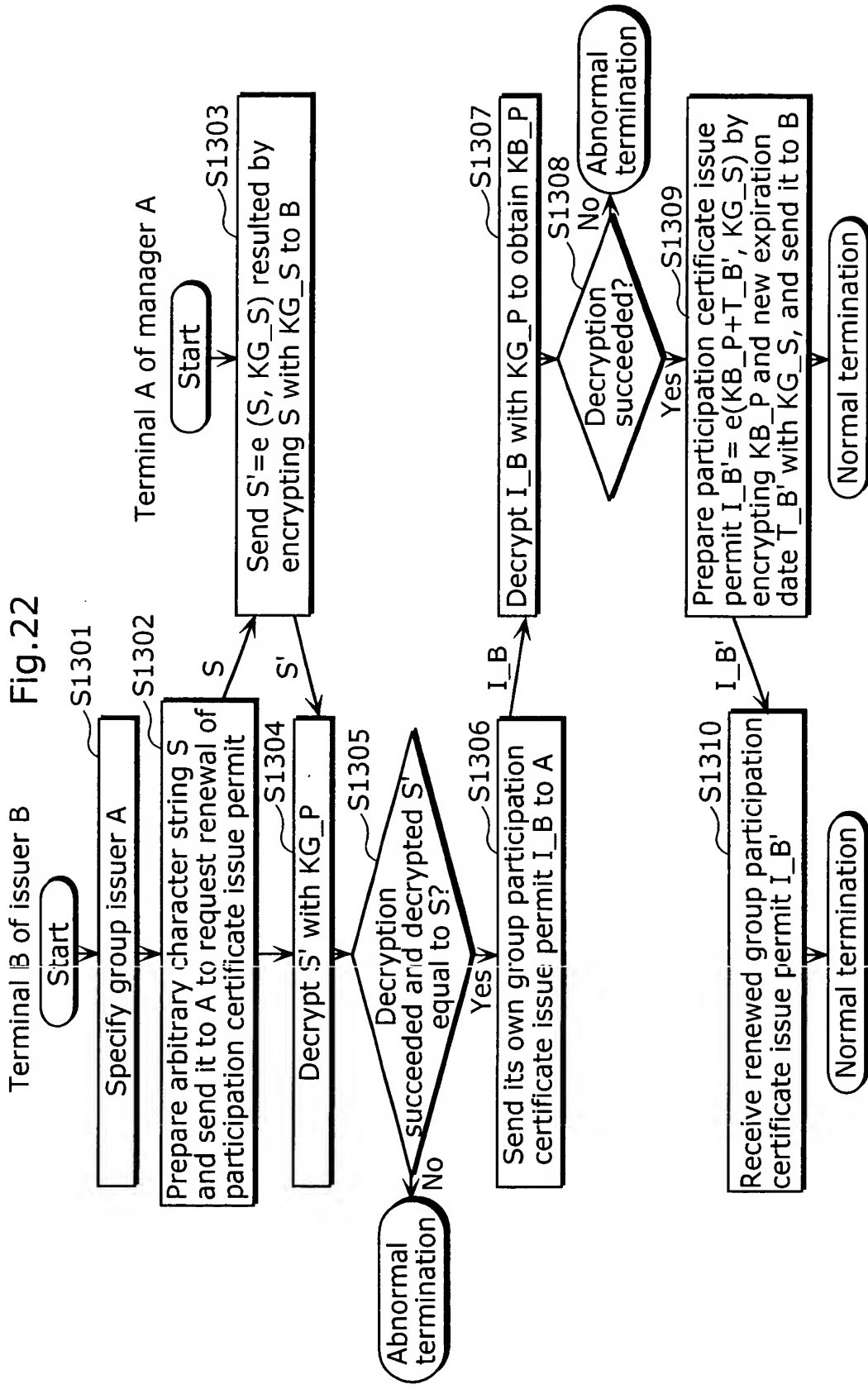


Fig.23

KB\_P:Public key of B  
KB\_S:Private key of B  
KG\_P:Group public key  
 $I_{B'} = e(KB_P + T_{B'}, KG_S)$   
:Group participation certificate issue permit of B

Fig.24

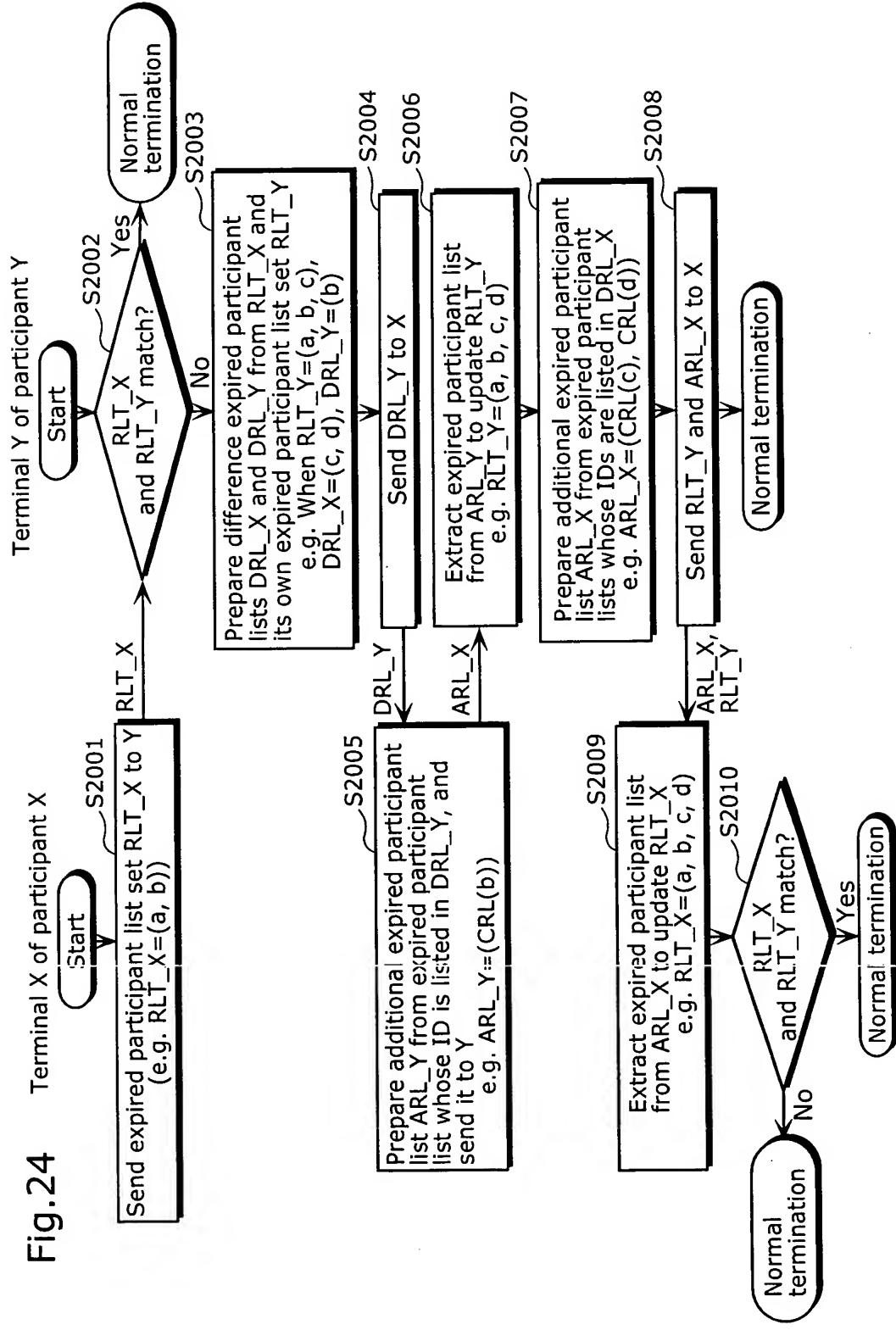


Fig.25

RLT\_X:Collection of expired participant lists (expired participant list set) possessed by X  
DRL\_X:Collection of expired participant lists (difference expired participant list) not possessed by X  
ARL\_X:Collection of expired participant lists (additional expired participant list) not possessed by X  
a, b,c, d, ...:Expired participant list ID  
CRL(a):Expired participant list whose ID is "a"



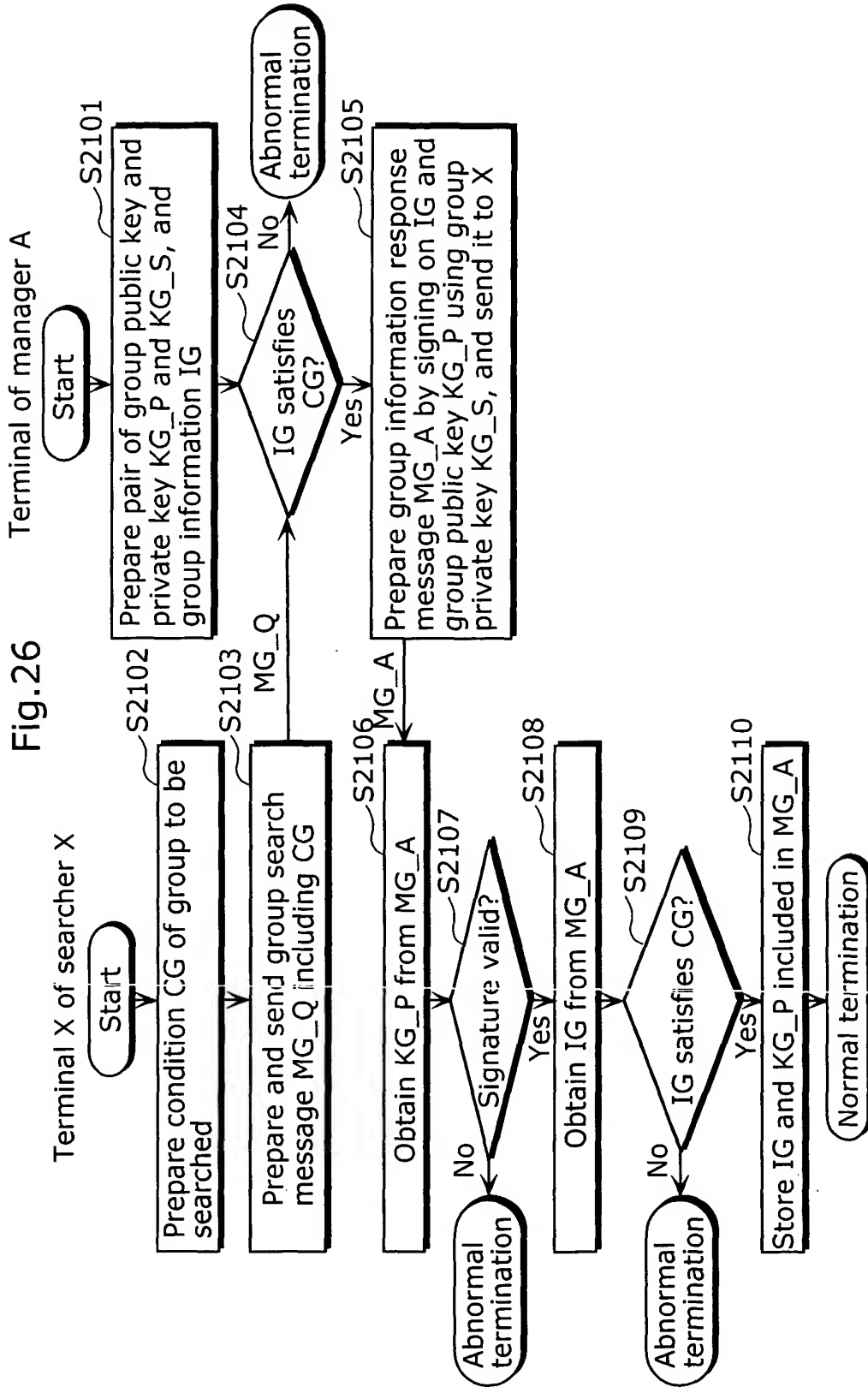


Fig.27

KG\_P: Group public key  
IG: Information about group  
(Category, information required for participation etc.)

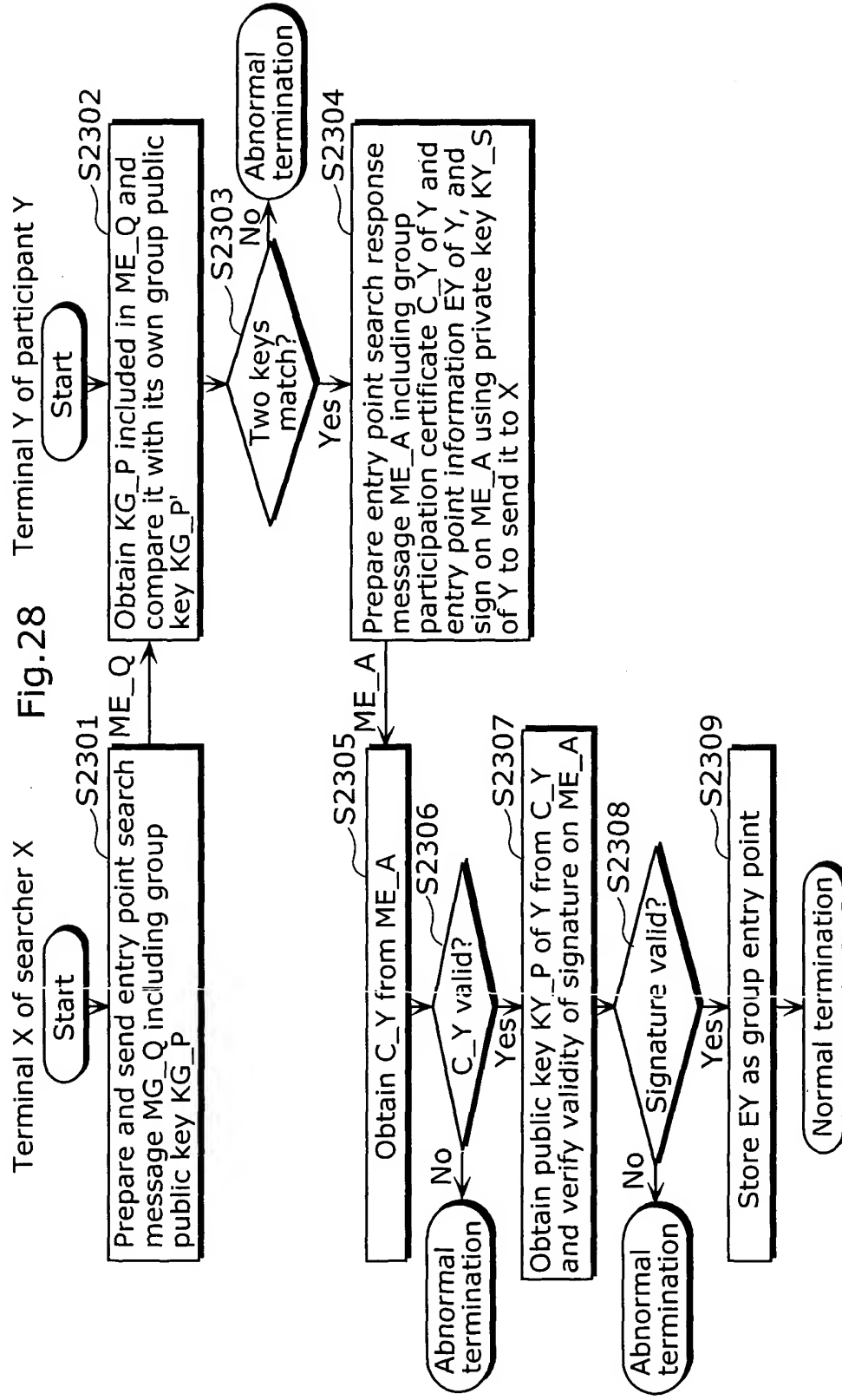


Fig.29

EY:Entry point information Y  
(IP address, port number etc.)  
C\_Y:Group participation certificate of Y

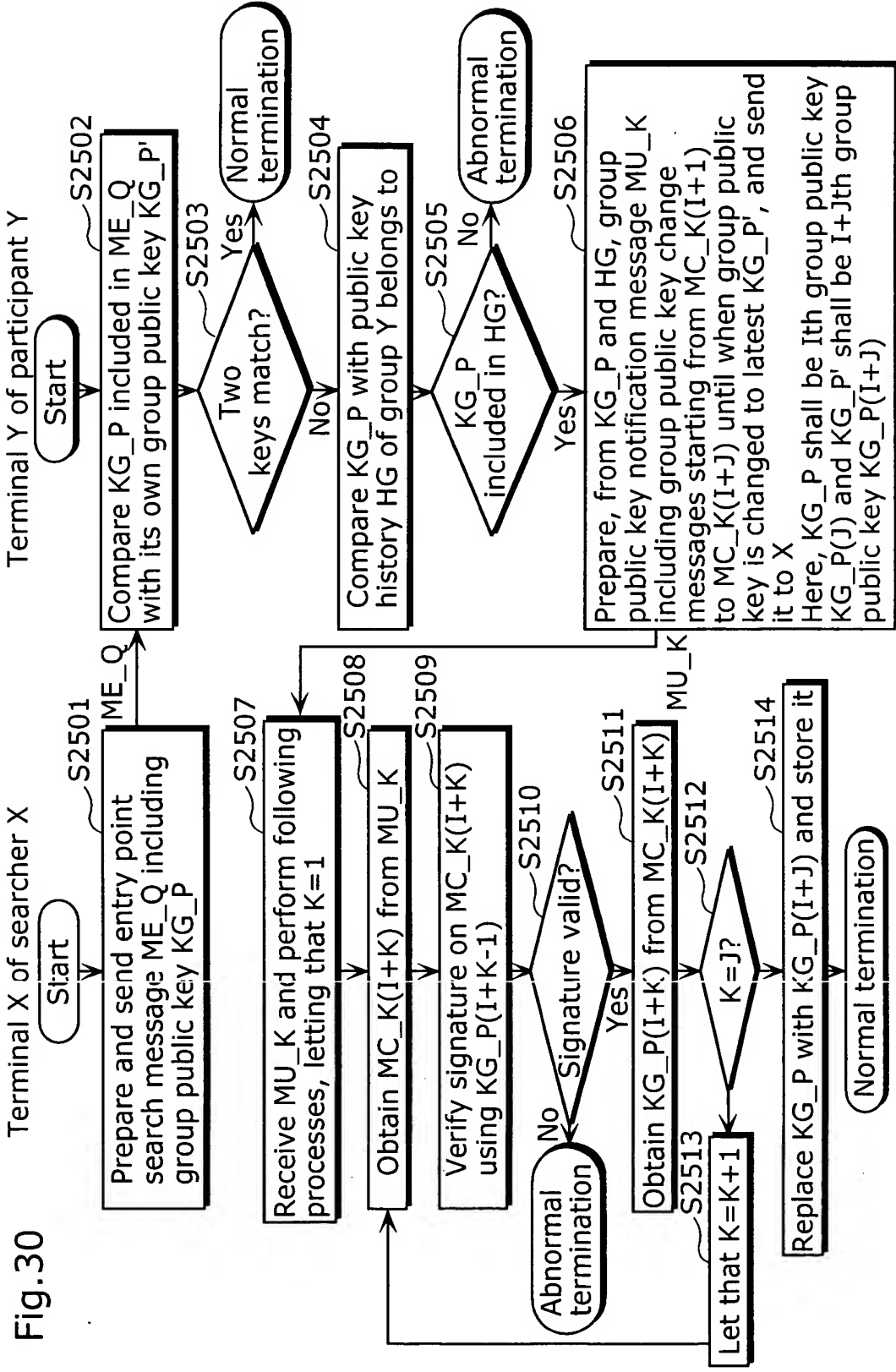
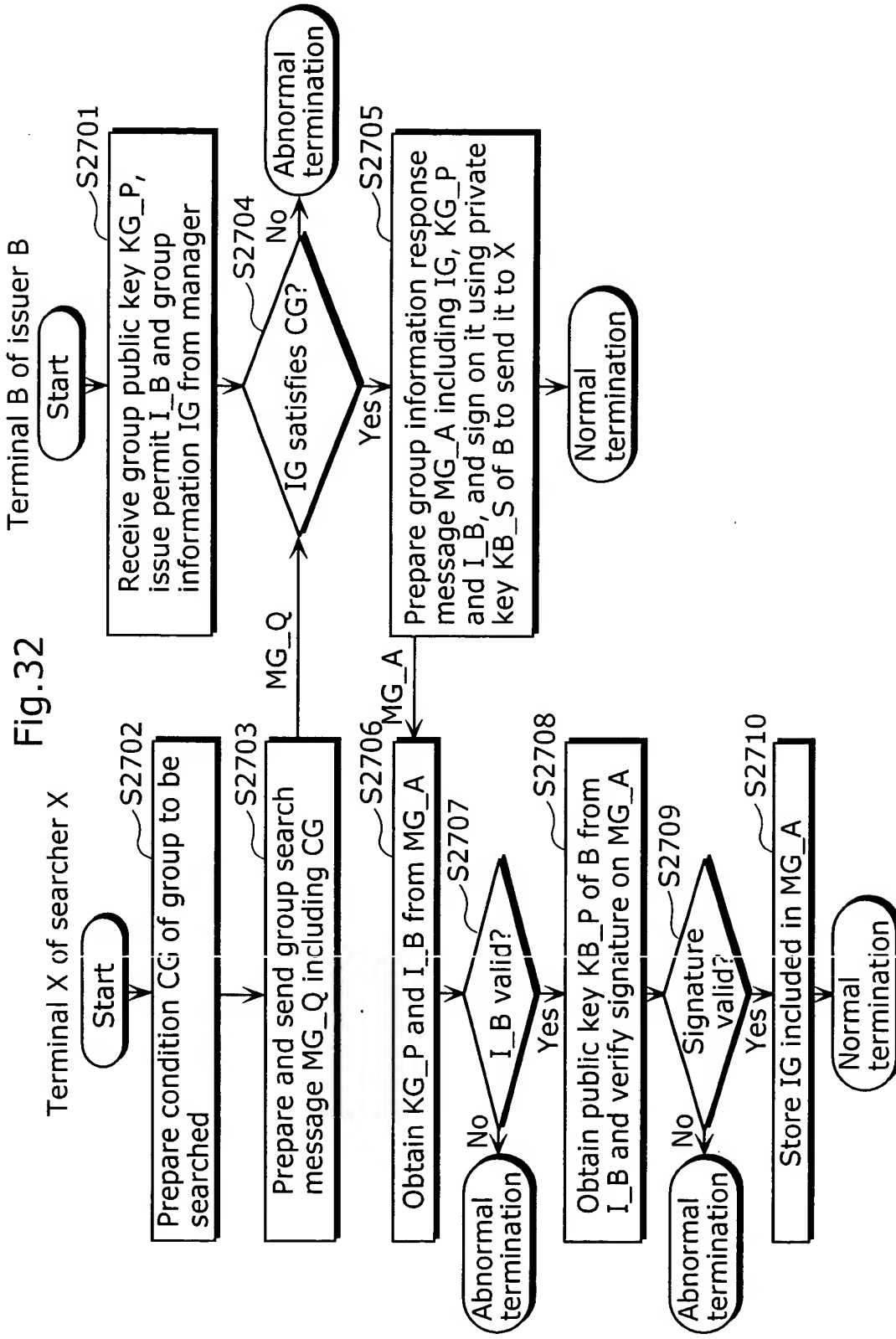


Fig.31

KG\_P':Latest group public key



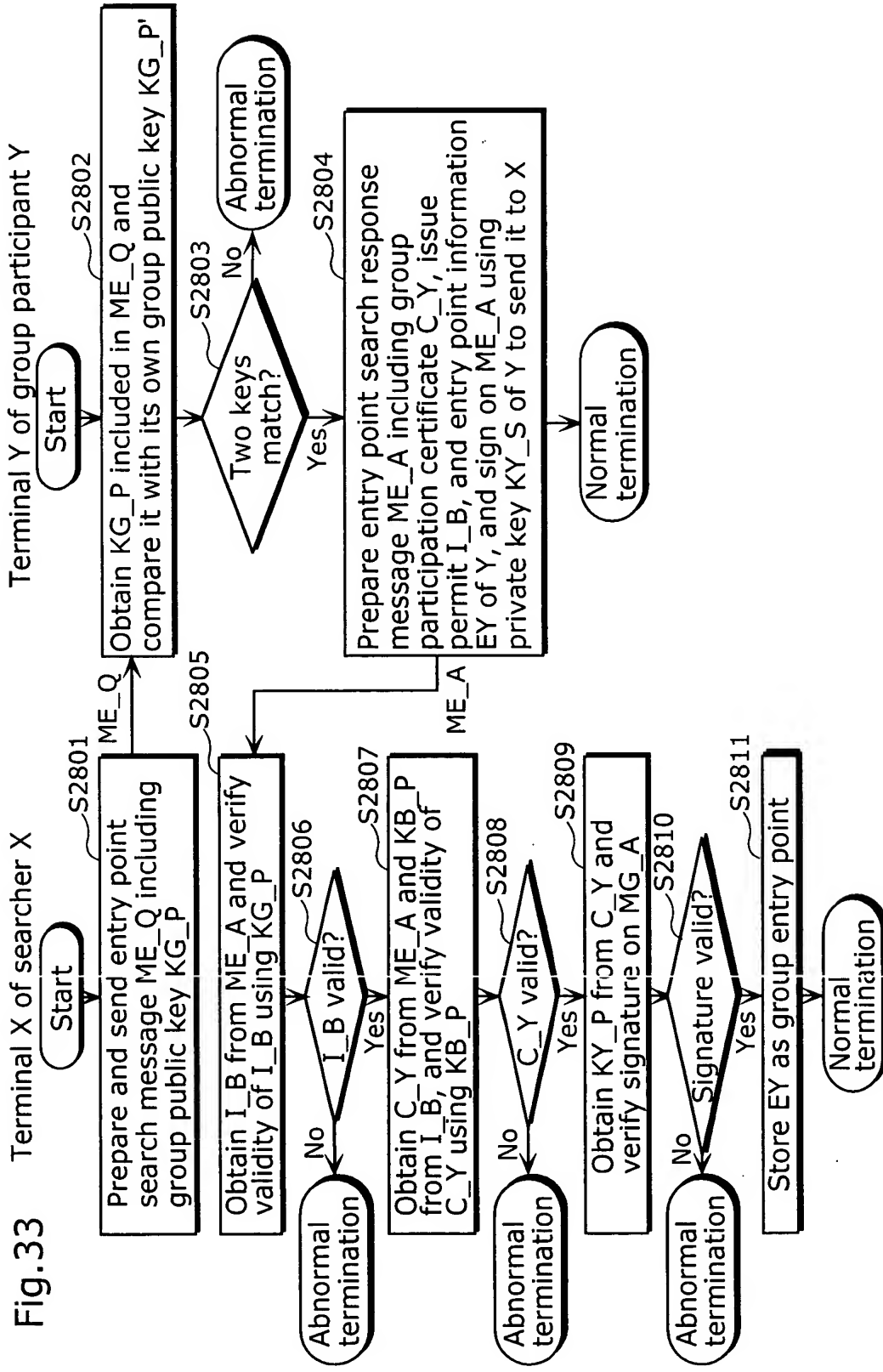




Fig.34

EY:Entry point information of Y  
(IP address, port number etc.)  
C\_Y:Group participation certificate of Y  
I\_B:Group participation certificate issue permit of B